Vol 16 No 4, April 2007
1009-1963/2007/16(04)/0910-05
Chinese Physics
© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

# An efficient two-step quantum key distribution protocol with orthogonal product states*

Yang Yu-Guang(杨宇光)[a)†], Wen Qiao-Yan(温巧燕)[b)], and Zhu Fu-Chen(朱甫臣)[c)]

[a)] *School of Computer, Beijing University of Technology, Beijing* 100022, *China*
[b)] *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[c)] *National Key Laboratory for Modern Communications, Chengdu* 610041, *China*

(Received 28 April 2006; revised manuscript received 2 November 2006)

An efficient two-step quantum key distribution (QKD) protocol with orthogonal product states in the $n \otimes n (n \geq 3)$ Hilbert space is presented. In this protocol, the particles in the orthogonal product states form two particle sequences. The sender, Alice, first sends one sequence to the receiver, Bob. After Bob receives the first particle sequence, Alice and Bob check eavesdropping by measuring a fraction of particles randomly chosen. After ensuring the security of the quantum channel, Alice sends the other particle sequence to Bob. By making an orthogonal measurement on the two particle sequences, Bob can obtain the information of the orthogonal product states sent by Alice. This protocol has many distinct features such as great capacity, high efficiency in that it uses all orthogonal product states in distributing the key except those chosen for checking eavesdroppers.

**Keywords:** quantum key distribution, orthogonal product state, orthogonal measurement
**PACC:** 0365, 4230

## 1. Introduction

Cryptography aims to transmit secret messages. With the development of quantum computation, especially the proposal of Shor's algorithm,[1] the basis of the most important classic cryptographic scheme was shocked. But at the same time, the principles of quantum mechanics have also shed new light on the field of cryptography as these fundamental laws guarantee the secrecy of quantum cryptosystems. Any intervention of an eavesdropper, Eve, must leave some trace which can be detected by the legal users of the communication channel. A lot of attention has been focused on QKD[2−14] since the BB84 QKD protocol was reported.[2]

In most of the existing QKD protocols, the participants choose randomly one of two sets of measuring bases (MBs), the intrinsic efficiency of these protocols is usually 50%. The favoured-measuring-basis technique[15] and the measuring-basis-encrypted technique[6] are used for improving intrinsic efficiency. Deng and Long proposed an order-rearrangement idea[16] for quantum key distribution. Long and Liu proposed a theoretical quantum key distribution scheme using blocks of Einstein–Podolsky–Rosen (EPR) pairs.[17]

In Ref.[7], Goldenberg and Vaidman first presented a quantum cryptographic scheme based on orthogonal states. Thereafter a quantum cryptographic scheme involving truly two orthogonal states was proposed.[10] The basic technique is to split the transfer of one-bit information into two steps, ensuring that only a fraction of the bit information is transmitted at a time. Guo *et al* proposed a novel quantum key distribution scheme with orthogonal product states.[18] In their scheme, the one particle in an orthogonal product state is transmitted only after the other particle has arrived the receiver. Then the no-cloning theorem of orthogonal states[19] guarantees its security.

In this paper, we present an efficient two-step quantum key distribution protocol with orthogonal product states in the $n \otimes n (n \geq 3)$ Hilbert space. In this protocol, the particles in the orthogonal product states are transmitted in a quantum data block. They form two particle sequences. The sender, Alice, first sends one sequence to the receiver, Bob. After

*Project supported by the National Natural Science Foundation of China (Grant No 60373059), the Doctoral Programs Foundation of the Ministry of Education of China (Grant No 20040013007), and the Major Research plan of the National Natural Science Foundation of China (Grant No 90604023).
†E-mail: yangyang7357@sina.com

Bob receives the first particle sequence, Alice and Bob check eavesdropping by measuring a fraction of particles randomly chosen. After ensuring the security of the quantum channel, Alice sends the other particle sequence to Bob. By making an orthogonal measurement on the two particle sequences, Bob can obtain the information of the orthogonal product states sent by Alice. Its intrinsic efficiency is improved to be 100%. Moreover, the classical information exchanged is reduced since the parties of communication need not to announce the information about the MBs in most instances. This protocol has many distinct features such as great capacity, and high efficiency.

## 2. Quantum key distribution protocol

For a $2 \otimes 2$ system, there are obviously no such orthogonal product states that satisfy the no-cloning theorem of orthogonal states. For simplicity and without loss of generality, we consider a $3 \otimes 3$ system.

For a $3 \otimes 3$ system, a general set of orthogonal product states in a Hilbert space are as follows:

$$\begin{aligned}
\Psi_1 &= |1\rangle_B(a|1\rangle_C + b|0\rangle_C),\\
\Psi_2 &= |1\rangle_B(b^*|1\rangle_C - a^*|0\rangle_C),\\
\Psi_3 &= (c|1\rangle_B - d|0\rangle_B)|2\rangle_C,\\
\Psi_4 &= (d^*|1\rangle_B - c^*|0\rangle_B)|2\rangle_C,\\
\Psi_5 &= |2\rangle_B(e|0\rangle_C + f|2\rangle_C),\\
\Psi_6 &= |2\rangle_B(f^*|0\rangle_C - e^*|2\rangle_C),\\
\Psi_7 &= (g|0\rangle_B + h|2\rangle_B)|1\rangle_C,\\
\Psi_8 &= (h^*|0\rangle_B - g^*|2\rangle_B)|1\rangle_C,\\
\Psi_9 &= |0\rangle_B|0\rangle_C, \qquad (1)
\end{aligned}$$

where $a, b, c, d, e, f, g, h$ are complex numbers and satisfy the normalization condition

$$|a|^2 + |b|^2 = |c|^2 + |d|^2 = |e|^2 + |f|^2 = |g|^2 + |h|^2 = 1.$$

Because the information is encoded in the orthogonal product states, to guard the secret information against eavesdropping, Alice cannot allow Eve to acquire simultaneously both particles in the orthogonal product states.

An ordered $N$ orthogonal product state sequence is denoted by $[(P_1(1); P_1(2)); (P_2(1); P_2(2)); \ldots; (P_i(1); P_i(2)); \ldots; (P_N(1); P_N(2))]$. We use $P_i(1)$ to denote one particle in the $i$th orthogonal product state, and $P_i(2)$ the other one, $i = 1; 2; \ldots; N$. We say that $P_i(1)$ is the partner particle of $P_i(2)$ and vice versa. The order of these $N$ orthogonal product states is maintained through out the QKD process. We can also take one partner particle $P_i(1)$ from each orthogonal product state $(P_i(1); P_i(2))$ to form an partner particle sequence $[P_1(1), P_2(1), P_3(1), \ldots, P_N(1)]$. The details of the protocol are as follows:

(i) Alice produces an ordered $N$ orthogonal product state sequence: $[(P_1(1); P_1(2)); (P_2(1); P_2(2)); \ldots; (P_i(1); P_i(2)); \ldots; (P_N(1); P_N(2))]$. Each orthogonal product state is randomly one of the nine orthogonal product states in Eq.(1).

(ii) Then Alice takes one particle from each orthogonal product state to form an ordered partner particle sequence: $[P_1(2), P_2(2), P_3(2), \ldots, P_N(2)]$. The rest of the partner particles form another ordered partner particle sequence: $[P_1(1), P_2(1), P_3(1), \ldots, P_N(1)]$. Alice sends to Bob one ordered partner particle sequence: $[P_1(2), P_2(2), P_3(2), \ldots, P_N(2)]$.

(iii) After Bob receives the ordered partner particle sequence, he chooses randomly a sufficiently large subset of the positions of particles and publishes the positions randomly chosen to Alice. Alice publishes the orthogonal product state which the two particles are in at each position. Then according to the announcement of Alice, Bob makes a corresponding orthogonal measurement and publishes his results. According to Bob's results, Alice makes the error rate analysis.

After that, if the error rate is less than $\varepsilon_1$, Alice and Bob can conclude that there are no eavesdroppers in the line. They should proceed to step (iv); otherwise they have to discard their transmission and abort the communication.

(iv) Alice sends to Bob the other ordered partner particle sequence: $[P_1(1), P_2(1), P_3(1), \ldots, P_N(1)]$.

(v)After receiving the two particle sequences, Bob makes orthogonal measurement on the two particle sequences on the basis in Eq.(1) simultaneously. Bob chooses randomly a subset of his results and compares them with Alice's. If the error rate is less than $\varepsilon_2$, Alice and Bob can consider no eavesdropper exists and continue to correct the errors in the results using error correction method. Otherwise, Alice and Bob abandon the transmission and repeat the procedures from the beginning.

As discussed above, Alice and Bob can ensure the security of the protocol and Eve will be found out if he eavesdrops the quantum channel.

## 3. Security of the QKD protocol

The proof of the security of our QKD protocol is based on the security for the transmission of the two particle sequences. The transmission and the security check of each of the two particle sequences in our QKD protocol are similar to the procedures in the extended BB84 QKD protocol based on encoding in a finite high-dimensional Hilbert space. Each particle sequence is an extension of BB84 protocol[2] from two bases, two-state encoding to multi bases, multi-state encoding. Our two-step QKD protocol is equal to the two extended BB84 QKD protocols where the two particles at the same position are in one of the nine orthogonal product states in Eq.(1).

Now, we evaluate the error rate and the correspondent maximal amount of information obtainable from an eventual eavesdropper as functions of the dimension of the Hilbert space while considering optimal incoherent eavesdropping attacks. We obtain the upper limit for the error rate to ensure unconditional security when the eavesdropper uses incoherent eavesdropping strategies.

In our QKD scheme, each particle in the first sequence is randomly in one of the seven states $\{a|1\rangle + b|0\rangle, b|1\rangle - a|0\rangle, |2\rangle, e|0\rangle + f|2\rangle, f|0\rangle - e|2\rangle, |1\rangle, |0\rangle\}$, with a probability of $\frac{1}{9}, \frac{1}{9}, \frac{2}{9}, \frac{1}{9}, \frac{1}{9}, \frac{2}{9}, \frac{1}{9}$, respectively. It is equal to an extension of BB84 protocol to three bases, three-state encoding. The three states in each of the three bases are $\{a|1\rangle + b|0\rangle, b|1\rangle - a|0\rangle, |2\rangle\}, \{e|0\rangle + f|2\rangle, f|0\rangle - e|2\rangle, |1\rangle\}, \{|0\rangle, |1\rangle, |2\rangle\}$, respectively.

Since the basis is unknown to the eavesdropper (by convention called Eve), she cannot simply clone the states sent by Alice because of the no-cloning theorem. The use of random complementary bases furthermore implies that if the sender Alice prepares a state in one basis, the outcome of measurement by Eve in a complementary basis will yield a totally random measurement outcome. These features guarantee that any eavesdropping attempt will invariably introduce errors in the transmission, which can be detected by the legitimate communicating parties.

Here we discuss an optimal individual eavesdropping strategy based on the use of an asymmetric version of the $N$-dimensional symmetric universal quantum cloning machine (UQCM) introduced by Bužek and Hillery.[20] This asymmetric cloning machine[21,22] can be used to obtain two copies of Alice's quantum state that are not of the same fidelity. Eve then keeps one of the copies (typically, the bad one) for herself, and passes the other copy (typically, the good one) to Bob. Then, after Alice has announced the orthogonal product states, Eve does the same measurement as Bob does, i.e., she measures her copy in the same basis as Bob. It should be stressed that, if Eve makes use of such an asymmetric UQCM for eavesdropping, she should exploit not only the state of her copy but also that of the cloning machine in order to extract a maximum of information on Alice's quantum state. In particular, she can make a coherent measurement on the state of the cloning machine and her copy in order to infer whether she introduces an error at Bob's station (and precisely what error).[23] Note that the quantum circuit that implements this asymmetric cloning machine is exhibited in Ref.[24].

Let us analyse the situation that Eve uses an $N$-dimensional cloning machine as described in Refs.[21,22]. If Alice sends the state $|\varphi_k\rangle$ of the particle in the first particle sequence, the output state is given by

$$|\varphi_k\rangle_A \to \sum_{m,n=0}^{N-1} a_{m,n} U_{m,n} |\varphi_k\rangle_B |\phi_{m,N-n}\rangle_{EM}, \quad (2)$$

where the amplitudes $a_{m,n} (m, n = 0, 1, \ldots, N-1)$ characterize the cloning machine and $A, B, E$ and $M$ stand for Alice, Bob, Eve and the cloning machine respectively. Here, the states $|\Phi_{m,n}\rangle_{EM}$ are the generalization of the Bell states, that is, a set of $N^2$ ortho-normal maximally-entangled states of two $N$-dimensional systems,

$$|\Phi_{m,n}\rangle_{EM} = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \mathrm{e}^{2\pi i (\ln/N)} |\varphi_l\rangle_E |\varphi_{l+m}\rangle_M, \quad (3)$$

where the indices $m$ and $n (m, n = 0, 1, \ldots, N-1)$ label the $N^2$ states. Note that, here and below, the ket labels take modulo $N$. The operators $|U_{m,n}\rangle$,defined as

$$|U_{m,n}\rangle = \sum_{k=0}^{N-1} \mathrm{e}^{2\pi i (kn/N)} |\varphi_{k+m}\rangle\langle\varphi_k|, \quad (4)$$

form a group of error operators on $N$-dimensional states, generalizing the Pauli matrices for qubits; $m$ labels the 'shift' errors (generalizing the bit flip $\sigma_x$) while $n$ labels the phase errors (generalizing the phase flip $\sigma_z$). Using the definition of the states $|\Phi_{m,n}\rangle$ and the operators $|U_{m,n}\rangle$, Eq.(2) can be rewritten as

$$|\varphi_k\rangle_A \rightarrow \frac{1}{\sqrt{N}}\sum_{m=0}^{N-1}|\varphi_{k+m}\rangle_B \times \sum_{l=0}^{N-1} c_{m,k-l}|\varphi_l\rangle_E|\varphi_{l+m}\rangle_M, \quad (5)$$

where

$$c_{m,j} = \sum_{n=0}^{N-1} a_{m,n}\mathrm{e}^{2\pi\mathrm{i}(jn/N)}. \quad (6)$$

Now, we suppose that the cloning machine described above is universal, that is[21,22]

$$a_{m,n} = \alpha\delta_{m,0}\delta_{n,0} + \frac{\beta}{N}, \quad (7)$$

with the normalization relation

$$\alpha^2 + \frac{2}{N}\alpha\beta + \beta^2 = 1, \quad (8)$$

where $\alpha$ and $\beta$ parameterize the asymmetry of the cloning machine. $c_{m,j}$ can be re-written as

$$c_{m,j} = \alpha\delta_{m,0} + \beta\delta_{j,0}, \quad (9)$$

so that we obtain for the cloning transformation

$$\begin{aligned}|\varphi_k\rangle_A \rightarrow & \frac{1}{\sqrt{N}}\sum_{m=0}^{N-1}|\varphi_{k+m}\rangle_B\left(\alpha\delta_{m,0}\sum_{l=0}^{N-1}|\varphi_l\rangle_E|\varphi_l\rangle_M + \beta|\varphi_k\rangle_E|\varphi_{k+m}\rangle\right)\\ = & |\varphi_k\rangle_B\left(\frac{\alpha}{\sqrt{N}}\sum_{l=0}^{N-1}|\varphi_l\rangle_E|\varphi_l\rangle_M + \frac{\beta}{\sqrt{N}}|\varphi_k\rangle_E|\varphi_k\rangle_M\right) + \sum_{m=1}^{N-1}|\varphi_{k+m}\rangle_B\left(\frac{\beta}{\sqrt{N}}|\varphi_k\rangle_E|\varphi_{k+m}\rangle_M\right). \quad (10)\end{aligned}$$

Eve's strategy is as follows. After Alice announces the orthogonal product states, Eve makes the same measurement on both her copy $E$ and the 'cloning machine' $M$ as Bob does. The probability of not being detected when Eve eavesdrops a particle is

$$\begin{aligned}p_s(1,N,\beta) &= p_{m=0}(k) + \sum_{l\neq k} p_{m=0}(l)\\ &= \frac{(\alpha+\beta)^2}{N} + (N-1)\frac{\alpha^2}{N}\\ &= 1 - \frac{N-1}{N}\beta^2. \quad (11)\end{aligned}$$

If $n$ particles are used for eavesdropping check, the probability of Eve not being detected is

$$p_s(n,N,\beta) = \left(1 - \frac{N-1}{N}\beta^2\right)^n. \quad (12)$$

To ensure the first particle sequence secure, $\varepsilon_1$ should be less than

$$1 - p_s(n,N,\beta) = 1 - \left(1 - \frac{N-1}{N}\beta^2\right)^n. \quad (13)$$

As shown in Ref.[20], the maximal fidelity of copying a quNit is obtained using the UQCM. This maximal value of the fidelity corresponds precisely to the fidelity of optimal incoherent eavesdropping strategy, as Bechmann-Pasquinucci and Gisin have shown explicitly for the $(N = 2; M = 3)$ case.[23]

If the error rate $\varepsilon_1$ is less than $1 - p_s(n,N,\beta) = 1 - \left(1 - \frac{N-1}{N}\beta^2\right)^n$, then Alice and Bob can consider that no eavesdropper exists in the transmission of the first particle sequence.

The eavesdropping check of the second particle sequence is similar to that of the first particle sequence. After the transmission of the two particle sequences, the probability of not being detected when Eve eavesdrops an orthogonal product state is $\left(1 - \frac{N-1}{N}\beta^2\right)^2$. For $n$ particle states used for eavesdropping check, the probability of Eve not being detected is $\left(1 - \frac{N-1}{N}\beta^2\right)^{2n}$.

To ensure the second particle sequence secure, $\varepsilon_2$ should be less than $1 - \left(1 - \frac{N-1}{N}\beta^2\right)^{2n}$.

## 4. Conclusion

In this paper, we have presented an efficient two-step quantum key distribution protocol with orthogonal product states in an $n \otimes n (n \geq 3)$ Hilbert space. In this protocol, the particles in the orthogonal product states are transmitted in a quantum data block. They form two particle sequences. The sender, Alice, first sends one sequence to the receiver, Bob. After Bob receives the first particle sequence, Alice and Bob

check eavesdropping by measuring a fraction of particles randomly chosen. After ensuring the security of the quantum channel, Alice sends the other particle sequence to Bob. Making an orthogonal measurement on the two particle sequences, Bob can obtain the information of the orthogonal product states sent by Alice. The intrinsic efficiency of the present protocol is improved to 100% as compared with others. Moreover, the classical information exchanged is reduced since the parties of communication need not to announce the information about the MB. This protocol has many distinct features such as great capacity, high efficiency, etc.

In our scheme, we need to store the checking sequence of photons for a while, to make eavesdropping check and wait for the second sequence of photons to come. This is the expense we have to pay to improve the intrinsic efficiency.

## References


[1] Shor P W 1994 *Proceedings* **35** Annual Symposium on Fundamentals of Computer Science (FOCS) 124

[2] Bennett C H and Brassad G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing,* Bangalore, India (IEEE, New York,) 175–179

[3] Ekert A 1991 *Phys. Rev. Lett.* **67** 661

[4] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[5] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[6] Hwang W Y, Koh I G and Han Y D 1998 *Phys. Lett.* A **244** 489

[7] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239

[8] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863

[9] Koashi M and Imoto N 1997 *Phys. Rev. Lett.* **79** 2383

[10] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893

[11] Guo G P, Li R, Guo G C 2001 *Phys. Rev.* A **64** 042301

[12] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **54** 3995 (in Chinese)

[13] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **54** 5544 (in Chinese)

[14] Yang Y G, Wen Q Y and Zhu F C 2005 *Acta Phys. Sin.* **54** 5549 (in Chinese)

[15] Deng F G, Zhou H Y and Long G L 2005 arxiv: quant-ph/0504119

[16] Deng F G and Long G L 2003 arxiv: quant-ph/0308172

[17] Long G L and Liu X S 2000 arxiv: quant-ph/0012056

[18] Guo G P, Li C F and Shi B S arxiv: quant-ph/0102060

[19] Mor T 1998 *Phys. Rev. Lett.* **80** 3137

[20] Bužek V and Hillery M 1998 *Phys. Rev. Lett.* **81** 5003

[21] Cerf N J 1998 *Acta Phys. Slov.* **48** 115

[22] Cerf N J 2000 *J. Mod. Opt.* **47** 187

[23] Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238

[24] Braunstein S L, Bužek V and Hillery M 2001 *Phys. Rev.* A **63** 052313